
University of Belgrade
Faculty of Mathematics
Automated Reasoning GrOup
Fourth Workshop on Formal and Automated Theorem Proving and Applications
Belgrade, February 4-5, 2011.
argo.matf.bg.ac.rs/events/2011/fatpa2011.html
Participants:
Milan Banković, University of Belgrade, Serbia
Silvia Ghilezan, University of Novi Sad, Serbia
Tihomir Gvero, EPFL, Lausanne, Switzerland
Hugo Herbelin, INRIA- PPS, Paris, France
Svetlana Jakšić, University of Novi Sad, Serbia
Predrag Janičić, University of Belgrade, Serbia
Oliver Kullmann, Swansea University, UK
Stevan Kordić, University of Montenegro, Montenegro
Petar Maksimović, Mathematical Institute, Belgrade, Serbia
Oded Maler, CNRS/Verimag, France
Marko Maliković, University of Rijeka, Croatia
Filip Marić, University of Belgrade, Serbia
Bojan Marinković, Mathematical Institute, Belgrade, Serbia
Walther Neuper, Graz University of Technology, Austria
Dejan Ničković, Institute of Science and Technology (IST), Austria
Mladen Nikolić, University of Belgrade, Serbia
Jovanka Pantović, University of Novi Sad, Serbia
Vesna Pavlović, University of Belgrade, Serbia
Danijela Petrović, University of Belgrade, Serbia
Ivan Petrović, University of Belgrade, Serbia
Nina Radojičić, University of Belgrade, Serbia
Ana Spasić, University of Belgrade, Serbia
Mirko Spasić, University of Belgrade, Serbia
Mirko Stojadinović, University of Belgrade, Serbia
Sana Stojanović, University of Belgrade, Serbia
Milan Todorović, University of Belgrade, Serbia
Milena Vujošević-Janičić, University of Belgrade, Serbia
Aleksandar Zeljić, University of Belgrade, Serbia
Organisation:
Automated Reasoning GrOup
University of Belgrade, Serbia
argo.matf.bg.ac.rs

Fourth Workshop on Formal and Automated Theorem Proving and Applications

http://argo.matf.bg.ac.rs/events/2011/fatpa2011/fatpa2011.html

Book of Abstracts

and

Little Belgrade City Guide for Workshop Participants

February 4-5, 2011, Belgrade, Serbia

Preface

This booklet contains abstracts of the talks given at the:

Fourth Workshop on Formal and Automated Theorem Proving and Applications

held at the University of Belgrade on February 4-5, 2011. The meeting was attended by 28 participants coming from 12 research institutions from 7 European countries (Austria (2), Croatia (1), France (2), Montenegro (1), Serbia (21), Switzerland (1), United Kingdom (1)).

The programme consisted of 21 presentations, divided (rather loosely) into the four categories: Theoretical computer science, Formal theorem proving and applications, Automated theorem proving and applications, Early stage work.

More details about the meeting can be found online: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/fatpa2011.html`

The meeting was organized by the ARGO group (`http://argo.matf.bg.ac.rs`). For the success of the meeting, we are grateful to all speakers and all participants. We are also grateful to the Faculty of Mathematics, University of Belgrade which was the host institution of the meeting.

Predrag Janičić,
Associate professor at the Faculty of Mathematics,
University of Belgrade, Serbia

Participants

1. Marija Aćimović (Microsoft Development Center Serbia, Serbia)
   `http://www.microsoft.com/scg/mdcs/default.mspx`
2. Milan Banković (University of Belgrade, Serbia)
   `http://www.matf.bg.ac.rs/~milan`
3. Silvia Ghilezan (University of Novi Sad, Serbia)
   `http://imft.ftn.ns.ac.rs/~silvia`
4. Tihomir Gvero (EPFL, Lausanne, Switzerland)
   `http://people.epfl.ch/tihomir.gvero`
5. Hugo Herbelin (INRIA — PPS, Paris, France)
   `http://pauillac.inria.fr/~herbelin/index-eng.html`
6. Svetlana Jakšić (University of Novi Sad, Serbia)
   `http://imft.ftn.uns.ac.rs/~svetlana/`
7. Predrag Janičić (University of Belgrade, Serbia)
   `http://www.matf.bg.ac.rs/~janicic`

8. Oliver Kullmann (Swansea University, United Kingdom)
   http://www.cs.swan.ac.uk/~csoliver/
9. Stevan Kordić (University of Montenegro, Montenegro)
10. Petar Maksimović (Mathematical Institute, Belgrade, Serbia)
11. Oded Maler (CNRS/Verimag, France)
    http://www-verimag.imag.fr/~maler/
12. Marko Maliković (University of Rijeka, Croatia)
    http://www.ffri.uniri.hr/index.php?option=com_people&Itemid=83&task=display&id=623
13. Filip Marić (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~filip
14. Bojan Marinković (Mathematical Institute, Belgrade, Serbia)
    http://www.mi.sanu.ac.rs/~bojanm/
15. Walther Neuper (Graz University of Technology, Austria)
    http://www.ist.tugraz.at/neuper
16. Dejan Ničković (Institute of Science and Technology (IST), Austria)
    http://pub.ist.ac.at/~nickovic/
17. Mladen Nikolić (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~nikolic
18. Vesna Pavlović (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~vesnap
19. Danijela Petrović (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~danijela/
20. Ivan Petrović (University of Belgrade, Serbia)
21. Nina Radojičić (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~nina/
22. Ana Spasic (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~aspasic/
23. Mirko Spasić (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~mirko
24. Mirko Stojadinović (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~mirkos
25. Sana Stojanović (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~sana
26. Milan Todorović (University of Belgrade, Serbia)
27. Milena Vujošević-Janičić (University of Belgrade, Serbia)
    http://www.matf.bg.ac.rs/~milena
28. Aleksandar Zeljić (University of Belgrade, Serbia)

Programme and Abstracts

Programme

February 4, 2011.

February 4, 2011.	
10:00—10:25	Registration
10:25—10:30	Opening Remarks
Session *Theoretical Computer Science*; Session Chair: Silvia Ghilezan	
10:30—11:30	Oded Maler (CNRS/Verimag, France): *The Potential Roles of Informatics in Systems Biology*
11:30—12:00	Coffee break
12:00—12:30	Hugo Herbelin (INRIA — PPS, Paris, France): *An Excursion Into the Proofs-as-programs Correspondence*
12:30—13:00	Dejan Ničković (Institute of Science and Technology, Austria): *From MTL to Deterministic Timed Automata*
13:00—13:30	Bojan Marinković (Mathematical Institute, Belgrade, Serbia): *Formal Description of the Chord Protocol using ASM*
13:30—15:00	Lunch break (Restaurant "Ljubić")
Session *Formal Theorem Proving and Applications*; Session Chair: Dejan Ničković	
15:00—15:30	Marko Maliković (University of Rijeka, Croatia): *Automated Reasoning about Retrograde Chess Problems using Coq*
15:30—16:00	Petar Maksimović (Mathematical Institute, Belgrade, Serbia): *Formal Verification of Key Properties for Several Probability Logics in the Proof Assistant Coq*
16:00—16:30	Coffee break
16:30—17:00	Walther Neuper (Graz University of Technology, Austria): *Geometry Construction Languages Guiding User-interaction via a Lucas-Interpreter*
17:00—17:30	Filip Marić (University of Belgrade, Serbia): *Verified Efficient Unsatisfiability Proof Checking for SAT*
19:30—22:00	Dinner at "Teatroteka"

February 5, 2011.

February 5, 2011.	
Session *Automated Theorem Proving and Applications*; Session Chair: Filip Marić	
10:00—10:30	Oliver Kullmann (Swansea University, United Kingdom): *How to Translate into SAT such that SAT Solvers Have a Good Time?!?*
10:30—11:00	Tihomir Gvero (EPFL, Lausanne, Switzerland): *Interactive Synthesis of Code Snippets*
11:00—11:30	Coffee break
11:30—12:00	Milan Banković (University of Belgrade, Serbia): *ArgoSMTExpression: SMT-LIB 2.0 Compliant Expression Library*
12:00—12:30	Milena Vujošević-Janičić (University of Belgrade, Serbia): *A New Verification Tool: From LLVM Code to SMT Formulae*
12:30—13:00	Mladen Nikolić (University of Belgrade, Serbia): *ArgoCaLyPso - SAT Inspired Coherent Logic Prover*
13:00—14:30	Lunch break (Restaurant "Ljubić")
Session *Applications*; Session Chair: Predrag Janičić	
14:30—15:00	Stevan Kordić and Nataša Kovač (University of Montenegro, Montenegro): *One Combinatorial Algorithm for Berth Allocation Problem*
15:00—15:30	MDCS Math team (Microsoft Development Center Serbia, Serbia): Some Recent Developments in MDCS
15:30—16:00	Coffee break
Session *Early Stage Work*; Session Chair: Predrag Janičić	
16:00—16:15	Vesna Pavlović (University of Belgrade, Serbia): *Solving Geometric Construction Problems*
16:15—16:30	Danijela Petrović (University of Belgrade, Serbia): *Automated Proving in Geometry using Gröbner bases in Isabelle/HOL*
16:30—16:45	Ivan Petrović (University of Belgrade, Serbia): *Java Implementation of Wu's Method for Automated Theorem Proving in Geometry*
16:45—17:00	Mirko Stojadinović (University of Belgrade, Serbia): *How Efficient Can Fully Verified Functional Programs be —* *a Case Study of Graph Traversal Algorithms*
17:00—17:15	Mirko Spasić (University of Belgrade, Serbia): *Formalizing Simplex within Isabelle/HOL*
17:15—17:30	Aleksandar Zeljić (University of Belgrade, Serbia): *Solving Some NP-complete Problems Instances by Reductions*
18:30—19:30	Mini guided tour: Knez Mihajlova Street
19:30—22:30	Dinner at Skadarlija (Restaurant "Zlatni bokal")

Theoretical Computer Science

Session Chair: Silvia Ghilezan

1 The Potential Roles of Informatics in Systems Biology

Oded Maler
CNRS/Verimag, France

Abstract

In this talk I argue that the role of informatics (CS) in the development of biology can be more profound than that of a useful material tool. The CS approach to dynamical systems, practiced in the domain of system verification, and its extension to timed and hybrid systems can contribute to the conceptual foundations of systems biology and give new insights absent in traditional mathematical and physical approaches.

Slides: http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/OdedMaler.pdf

---

2 An Excursion Into the Proofs-as-programs Correspondence

Hugo Herbelin
INRIA — PPS, Paris, France

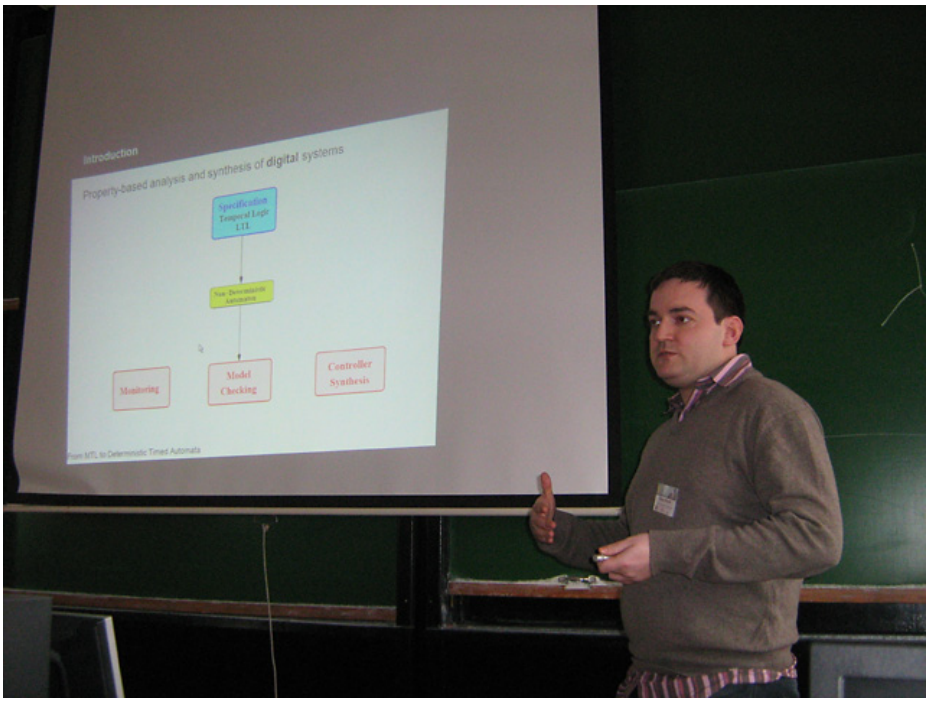
Abstract

We propose an excursion through the relation between proofs and programs that we keep discovering that it is tighter and tighter than we thought. Starting from Brouwer's manifesto that intuitionistic proof are effective, we will remind the main steps of the story: Kleene's realisability as an effective way to compute with intuitionistic proofs, Curry's revelation, followed by Howard's one, that proofs syntactically coincide with programs, Martin-Lf's type theory as a striking application of Howard's correspondence, Griffin's new revelation that classical logic computes too, after what, new achievements came such as computing with the sequent calculus, with the axiom of dependent choice, with Markov's principle, or even maybe, as Krivine and Miquel are currently investigating it, computing with axioms such as the continuum hypothesis (or its negation).

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/HugoHerbelin.pdf`

---

3 From MTL to Deterministic Timed Automata



Dejan Ničković
Institute of Science and Technology (IST), Austria

Abstract

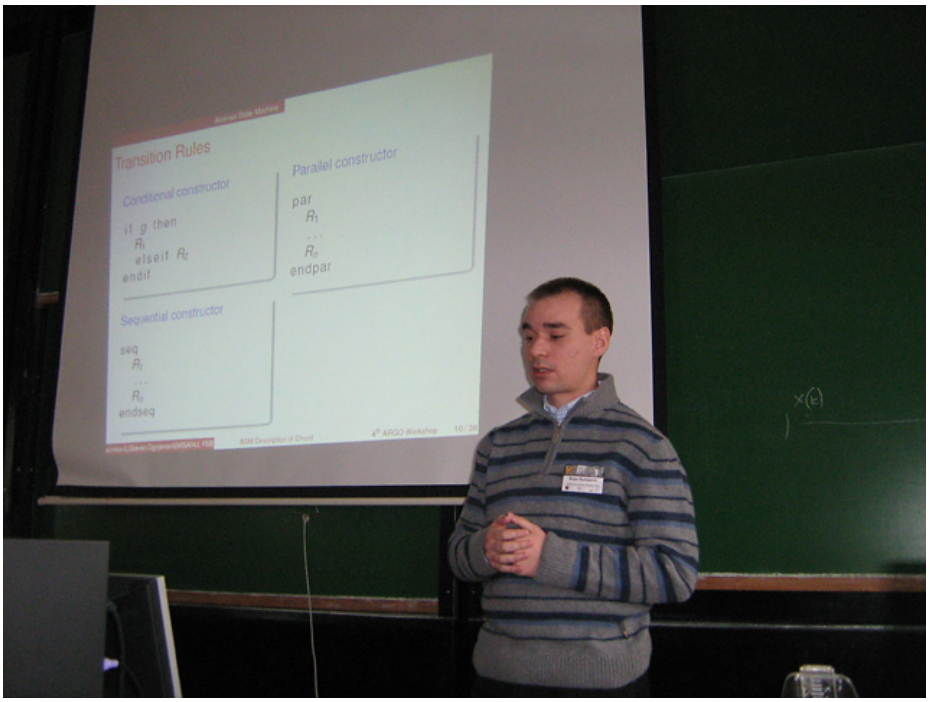
In this talk we propose a novel technique for constructing timed automata from properties expressed in the logic MTL, under bounded-variability assumptions. We handle full MTL and include all future operators. Our construction is based on separation of the continuous time monitoring of the input sequence and discrete predictions regarding the future. The separation of the continuous from the discrete allows us to determinize our automata in an exponential construction that does not increase the number of clocks. This leads to a doubly exponential construction from MTL to deterministic timed automata, compared with triply exponential using existing approaches.

We offer an alternative to the existing approach to linear real-time model checking, which has never been implemented. It further offers a unified framework for model checking, runtime monitoring, and synthesis, in an approach that can reuse tools, implementations, and insights from the discrete setting.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/DejanNickovic.pdf`

---

4 Formal Description of the Chord Protocol using ASM



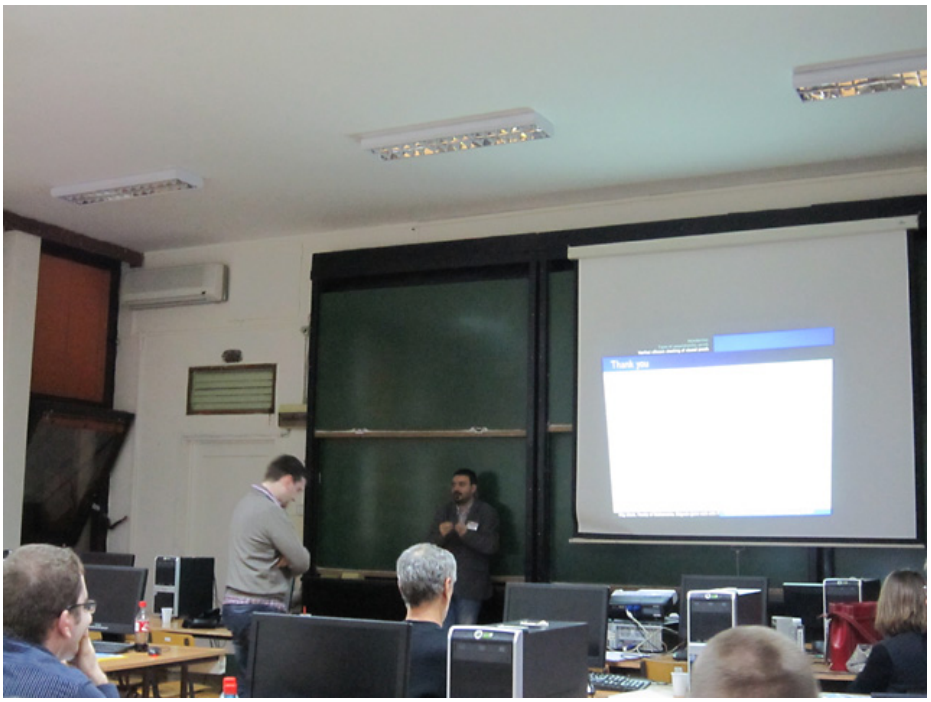
Bojan Marinković
Mathematical Institute, Belgrade, Serbia

Abstract

During this talk we will describe the overlay protocol Chord using the formalism of Abstract State Machine. The formalization concerns Chord actions that maintain ring topology and manipulate distributed keys. We will prove the correctness of our formalization. This is the join work with Paola Glavan (Faculty od Mechanical Engineering and Naval Architecture, Croatia) and Zoran Ognjanovic (Mathematical Institute of the Serbian Academy of Sciences and Arts), and it is submitted for the RTA 2011 conference.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/BojanMarinkovic.pdf`

Formal Theorem Proving and Applications



Session Chair: Dejan Ničković

5 Automated Reasoning about Retrograde Chess Problems using Coq

Marko Maliković
University of Rijeka, Croatia

Abstract

Retrograde chess analysis is a method that determines which moves have to be (or could be) played leading up to a given chess position. Retrograde chess analysis can be used for different purposes. There are several main types of retrograde chess problems that require different methods in order to be solved. In this workshop, I will describe the work we have done using Coq for automated reasoning about retrograde chess problems, from a basic formal system that includes axioms, definitions, hypotheses, functions, etc., through methods for generating required (possible) retrograde chess moves, up to a number of heuristic solutions for solving problems within a large search space such as retrograde chess analysis.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/MarkoMalikovic.pdf`

---

6 Formal Verification of Key Properties for Several Probability Logics in the Proof Assistant Coq

Petar Maksimović
Mathematical Institute, Belgrade, Serbia

Abstract

We present an encoding of four probability logics in the proof assistant Coq. These logics allows for reasoning on the probability of events, with and without iterations of probability operators, using a finitely-valued or a rational measure. We encode their syntax, semantics, and axiom systems, and provide formal proofs of some important meta-theorems, notably soundness, strong and simple completeness, and compactness. This represents a first step toward a formally certified probabilistic SAT-checker.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/PetarMaksimovic.pdf`

---

7 Geometry Construction Languages Guiding User-interaction via a Lucas-Interpreter

Walther Neuper
Graz University of Technology, Austria

Abstract

The talk considers issues in combining two technologies, 'Geometry Construction Languages' (GCLs) and 'Lucas Interpreters' (PLIs).

GCLs are designed to do what their name announces, in science and in education (the latter use is addressed by the combination); advanced GCLs integrate computation and deduction.

A PLI shifts user-interaction from the programming language (the GCL) to the interpretation of a program written in that language: like a debugger a PLI steps from breakpoint to breakpoint, where the breakpoints are at the statements adding a geometric object to the construction. And at the breakpoint the user (= student) gains full control over the respective construction.

The talk addresses this challenging question: What kinds of input by the user allows a PLI to resume execution of a program (i.e to continue user guidance)?

We shall see, that very general answers seem possible, if the PLI works on GCLs integrating computation and deduction: 'Contexts' (in the narrow sense of Isabelle/Isar) integrate data contained in a traditional environment with logical data. So contexts provide all data an appropriate prover requires to accomplish this final task: proof (or disproof) that the finished construction fulfills the postcondition. A PLI handling intermediate steps seems to require some notion of 'equivalence of contexts', which shall also be discussed in the talk.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/WaltherNeuper.pdf`

8 Verified Efficient Unsatisfiability Proof Checking for SAT

Filip Marić
University of Belgrade, Serbia

Abstract

In order to be used in real-world applications, SAT solvers must be trusted. One of the main approaches for achieving trusted solvers is to make solvers emit evidences for their claims (models for satisfiable and proofs for unsatisfiable instances), and checking these evidences by independent tools. Usual unsatisfiability proofs are series of resolution steps and they can be checked by very simple tools, but they usually consume much space and it is not always easy to modify SAT solvers so that they can emit this kind of proofs. Alternative proofs are so called clausal proofs. They usually consume significantly less space and they can be easily emitted by most modern SAT solvers. However, if efficient proof checking is required, tools that can check clausal proofs have to be rather complex and the question arises how can these tools be trusted. In this work we present a proof checker for clausal proofs implemented in Isabelle/HOL. Our preliminary experiments show that this fully verified checker manages to achieve the desired level of efficiency.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/FilipMaric.pdf`

Automated Theorem Proving, SAT, SMT, Applications

Session Chair: Filip Marić

9 How to Translate into SAT such that SAT Solvers Have a Good Time?!?

Oliver Kullmann
Swansea University, United Kingdom

Abstract

In my talk in want to present some methods for translating hard problems into SAT in such a way that the problems become as easy as possible for solvers.

From non-boolean domains to the boolean domain, we developed the "generic translation", generalising the known "direct" and "logarithmic" translation, and which was successfully applied in [1] to problems from Ramsey theory. I would like to make that scheme better known, since likely it can be applied in many situations, and significant speed-ups of SAT solving can be gained.

Within the realm of boolean problems, we are investigating attacking AES via SAT, and I want to discuss methods and insights regarding the formulation of such a problem as a SAT problem.

The focus of our investigations are (really) hard problems, and where good translations shall help with (drastically) reducing running times of many years (or much more).

[1] Green-Tao Number and SAT, Oliver Kullmann, SAT 2010, LNCS 6175, pages 352-362. `http://www.springerlink.com/content/x6p3850762677260/`

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/OliverKullmann.pdf`

---

10 Interactive Synthesis of Code Snippets

Tihomir Gvero
EPFL, Lausanne, Switzerland

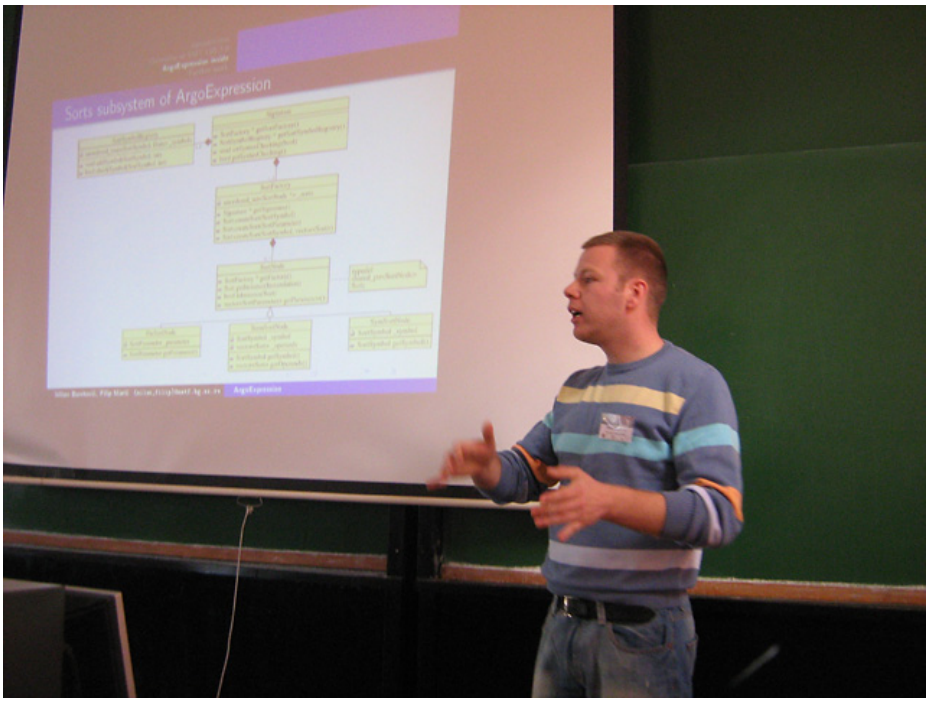
Abstract

We describe a tool that applies theorem proving technology to synthesize code fragments that use given library functions. Our approach takes into account polymorphic type constraints as well as code behavior. We have found our system to be useful for synthesizing code fragments for common programming tasks, and we believe it is a good platform for exploring software synthesis techniques. The tests that we ran indicate that our system scales well.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/TihomirGvero.pdf`

---

11 ArgoSMTExpression: SMT-LIB 2.0 Compliant Expression Library



Milan Banković
University of Belgrade, Serbia

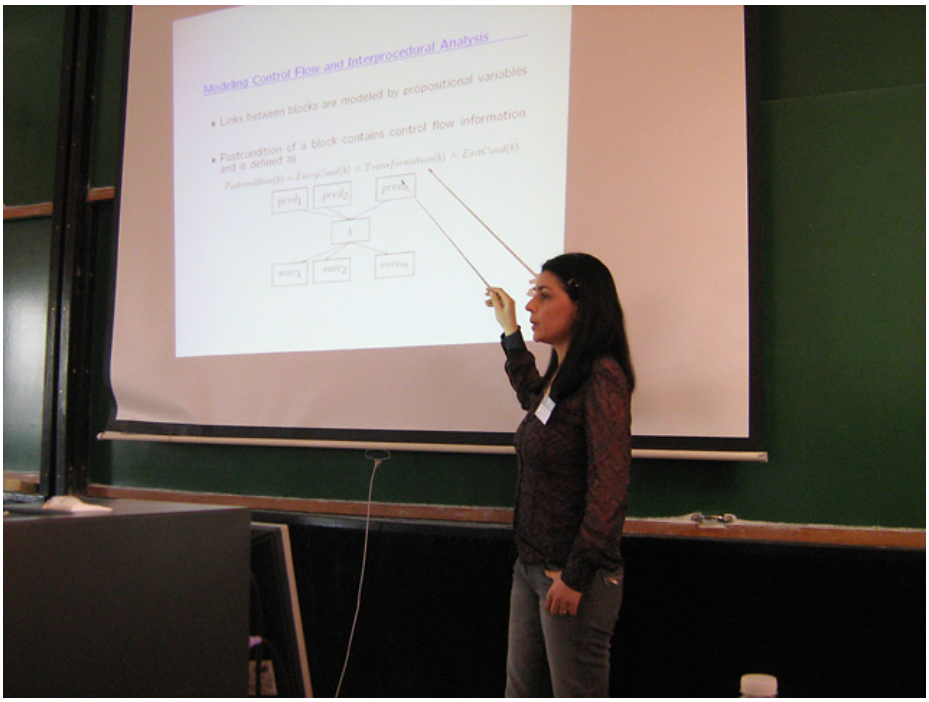
Abstract

SMT-LIB is an international initiative with a goal to provide a standard for describing background theories used in SMT in a rigorous manner, as well as input and output languages used in SMT systems. This includes a grammar for SMT expressions and formulae. The standard has been developed by Cesare Tinelli, Clark Barrett and Aaron Stump, with significant contribution of other SMT researchers and developers. Current version of SMT-LIB is 2.0, and it is still in active development. The first issue in developing an SMT-LIB compliant SMT solver is to provide a library for representing first-order expressions that supports all of SMT-LIB features. In this talk, our implementation of SMT-LIB-2.0 compliant expression library will be presented. It is still in active development, but it currently supports majority of SMT-LIB-2.0 features, including sort and function symbol declarations, sort terms, well-sortedness checking, term annotations, attributes, and so on. It is programmed in C++ and it will be released under GNU-GPL license. We hope that it would be useful for many others, and looking forward for cooperation and contribution of other interested researchers.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/MilanBankovic.pdf`

---

12 A New Verification Tool: From LLVM Code to SMT Formulae



Milena Vujošević-Janičić
University of Belgrade, Serbia

Abstract

A new approach and a corresponding tool for bug finding and for checking correctness conditions is going to be presented. The system works over LLVM code so it can be used for analysis of programs in several programming languages. The approach combines symbolic execution, SAT encoding of program's behavior and some features of bounded model checking. Namely, single blocks of the code are modelled by first-order logic formulae constructed by symbolic execution while relationships between blocks are modelled by propositional formulae. Formulae that describe program's behavior are combined with correctness conditions for individual commands to produce correctness conditions of the program to be verified. These conditions are passed to a SMT solver covering a suitable combination of theories. Currently, there is support for the following SMT solvers: Boolector, MathSAT, Yices, and Z3.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/MilenaVujosevicJanicic.pdf`

---

13 ArgoCaLyPso - SAT Inspired Coherent Logic Prover

Mladen Nikolić
University of Belgrade, Serbia

Abstract

Over the years, SAT solvers have exhibited significant jumps in performance thanks to several algorithmic improvements. However, not all of these improvements are limited to SAT domain. We present a new prover for coherent logic - ArgoCalypso. Distinguishing feature of this prover and the main goal of this work is development of SAT-like techniques in order to reinforce forward chaining — the standard approach to coherent logic proving. Positive indications are observed in preliminary testing of the prover.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/MladenNikolic.pdf`

---

14 One Combinatorial Algorithm for Berth Allocation Problem

Stevan Kordić and Nataša Kovač
University of Montenegro, Montenegro

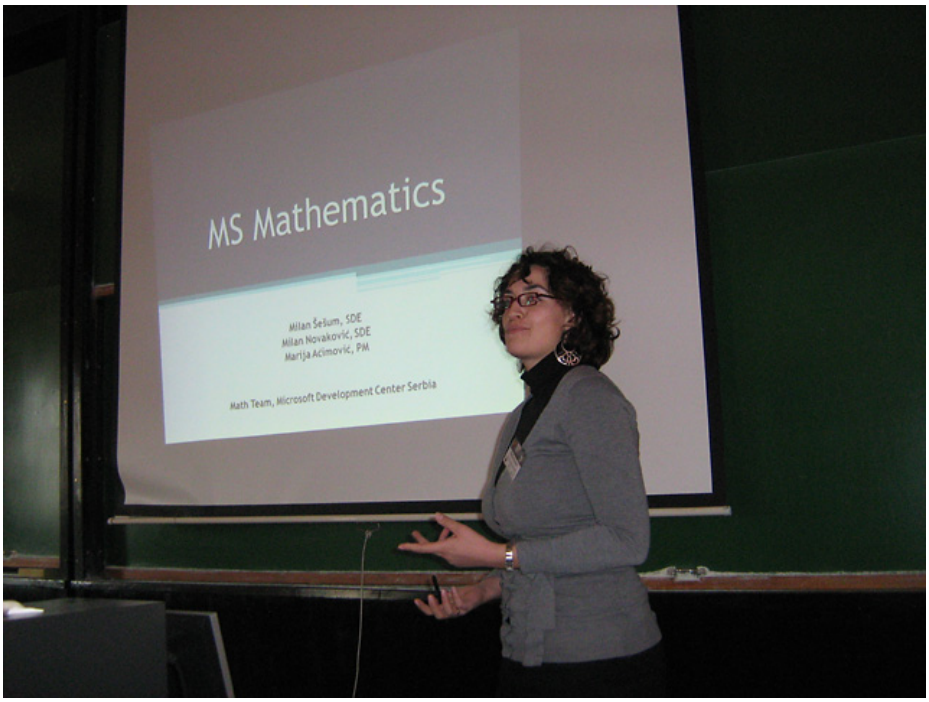
Abstract

Berth Allocation Problem is one of the fundamental problems of container terminal modeling. For the given berth layout and a set of vessels that have to be served within planning horizon optimal schedule should be made (optimal in terms of minimization of the penalties payed by port). It has been shown to be an NP-hard problem. Proposed exhaustive combinatorial algorithm use backtracking and a couple of look ahead techniques for solving of BAP.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/StevanKordic.pdf`

---

15 Some Recent Developments in MDCS



MDCS Math team
Microsoft Development Center Serbia, Serbia

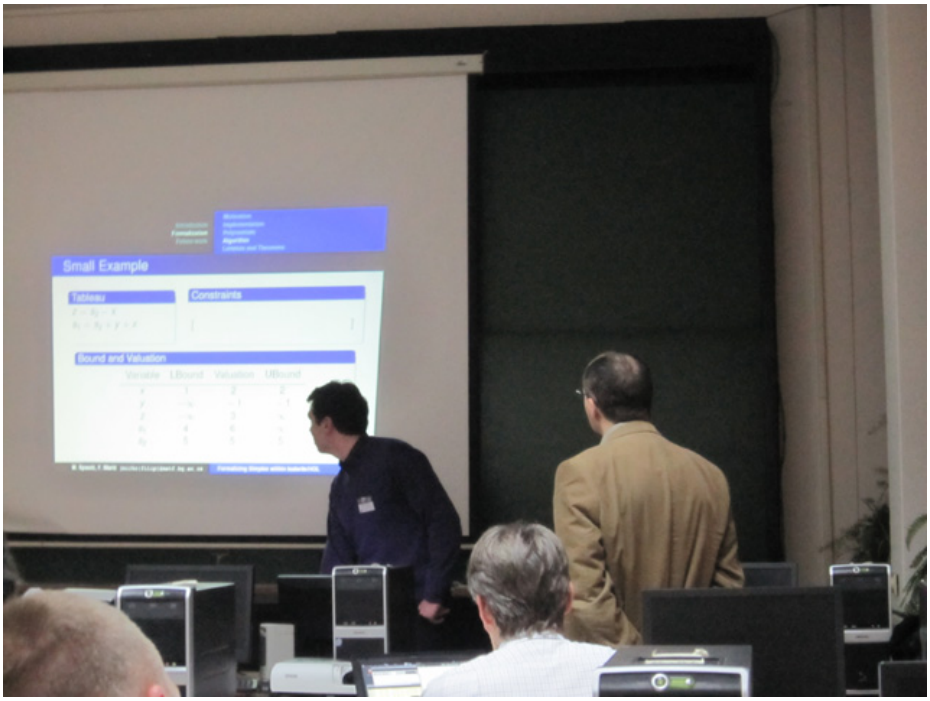
Abstract

MDCS (Microsoft Development Center Serbia) has recently shipped two products in the educational space: Mathematics Add-In for Microsoft Word and Microsoft OneNote, as well as a stand-alone application Mathematics 4.0. Both were developed primarily in Development Center in Belgrade, and are free for download from Microsoft Download Center.

Math team from MDCS will use this opportunity to present both of the products, as well as unique challenges that they faced during development. This will be an introduction into sharing experiences on software development in general, covering all phases of the software development lifecycle, from functional specifications to testing, UI design, instituting no-compromise quality assurance process and best practices in software design. This whole story will not remain in the realm of theory, but will be accompanied with demos showcasing the important details, as well as our plans and ideas for future projects.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/Microsoft.pdf`

Early Stage Work



Session Chair: Predrag Janičić

16 Solving Geometric Construction Problems

Vesna Pavlović
University of Belgrade, Serbia

Abstract

Automating geometry constructions is an important, but a hard task. So far there have not been many successful approaches for this problem.

In this talk we propose a method to construction a triangle given some of its elements. The approach combines forward and backward chaining and enables search for a construction both from objects that are known, as well as from objects that are sought to be constructed. An implementation is made in Prolog where rules correspond to elementary constructions. Currently, the program is able to produce analysis of a construction for some simpler problems. For future work, we are aiming at transition to resolution and the Vampire prover, and use of Gröbner bases for extraction of proof of construction and for identifying degenerate conditions.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/VesnaPavlovic.pdf`

---

17 Automated Proving in Geometry using Gröbner bases in Isabelle/HOL

Danijela Petrović
University of Belgrade, Serbia

Abstract

In Euclid geometry objects and relations between them can be expressed as polynomials. Further, any geometry construction can be expressed by set of polynomials and geometry statements can be proved by using the Gröbner bases method over that set of polynomials. We describe an implementation of an algorithm in Isabelle/HOL that accepts a term representation of a geometry construction and returns its corresponding set of polynomials. Our further work will be to use the method of Gröbner bases within Isabelle system on the generated polynomials, in order to prove correctness of the given construction.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/DanijelaPetrovic.pdf`

---

18 Java Implementation of Wu's Method for Automated Theorem Proving in Geometry

Ivan Petrović
University of Belgrade, Serbia

Abstract

In this talk we will present our ongoing work on Java implementation of the Wu's method for automated theorem proving in geometry. Our starting point is a C++ implementation of the method that is a part of the geometry tool GCLC. One of the main goals of this work is to develop an implementation of Wu's method that can be easily integrated in different dynamic geometry tools, such as GeoGebra.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/IvanPetrovic.ppt`

---

19 How Efficient Can Fully Verified Functional Programs be — a Case Study of Graph Traversal Algorithms

Mirko Stojadinović
University of Belgrade, Serbia

Abstract

One approach in achieving fully verified software is *shallow embedding* which assumes formalizing the software within a proof assistant, proving its total correctness, and exporting the executable code in a functional programming language by means of *code generation*. In order to be applicable for the real world applications, the generated code must be efficient. Concept of monads in functional programming enables using data structures and operation sequencing similar to those used in imperative languages, making the functional code more efficient. *Imperative HOL* is a new framework for the proof assistant *Isabelle/HOL* that enables code generation, employing monadic features. In this work we evaluate how efficient can generated code be, by doing a case study of graph algorithms. First, we implement *BFS (Breadth first search)* algorithm in Imperative HOL, prove its correctness and export code to a functional language (SML). Then we compare efficiency of this program to one written in an imperative language (C).

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/MirkoStojadinovic.pdf`

---

20 Formalizing Simplex within Isabelle/HOL

Mirko Spasić
University of Belgrade, Serbia

Abstract

In this work we formalize a Simplex-based linear arithmetic solver used within most state-of-the art SMT solvers. This procedure can be integrated in the DPLL(T) framework for SMT and is capable of deciding the satisfiability of conjunctions of linear constraints over reals. Our goal is to prove correctness for this decision procedure, within the Isabelle/Isar theorem proving system. From the logical specification in Isabelle, an effective executable code in functional programming languages can be generated.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/MirkoSpasic.pdf`

---

21 Solving Some NP-complete Problems Instances by Reductions

Aleksandar Zeljić
University of Belgrade, Serbia

Abstract

Solvers for some NP-complete problems (e.g. for SAT) achieved significant progress in recent years. However, it is not likely that problem-specific solvers for many NP-complete problems will follow that success. Hence, it is interesting to analyse efficiency of the problem solving based on reduction to other NP-complete problems and using solvers for those problems. Namely, reductions between NP-complete problems require polynomial time, but these reductions often yield impractical solutions. Since a wide range of combinatorial problems can be solved by reduction to some NP-complete problem, findings in reductions could potentially point to solvers for some other theory that might be better suited for some domains.

With the above motivation, we are planning to identify classes of formulas for which solvers for other problems can be practically used. We will also explore whether "hardest (random) instances" for one problem translate to "hardest instances" of the target problem. Currently we are focused on SAT and the clique problem and our preliminary findings will be presented.

Slides: `http://argo.matf.bg.ac.rs/events/2011/fatpa2011/slides/AleksandarZeljic.pdf`

Workshop Photos

Working session, February 04, 2011.

Dinner at Teatroteka, February 04, 2011.

Dinner at Teatroteka, February 04, 2011.

Dinner at Teatroteka, February 04, 2011.

Working session, February 05, 2011.

Lunch at Ljubić, February 05, 2011.

Guider Tour around Knez Mihajlova street, February 05, 2011.

Guider Tour around Knez Mihajlova street, February 05, 2011.

Guider Tour around Knez Mihajlova street, February 05, 2011.

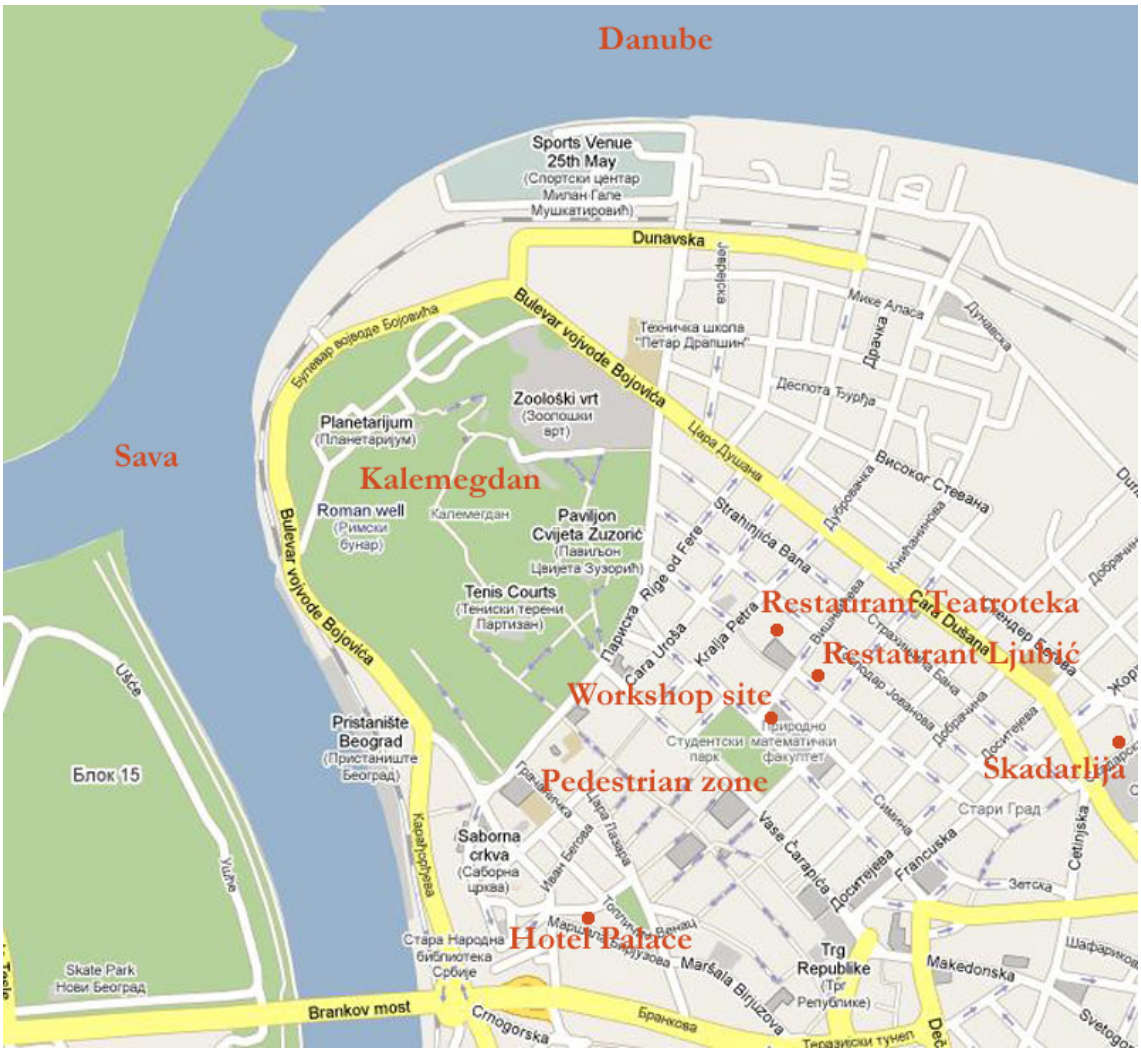
Dinner at Golden Jug in Skadarlija, February 05, 2011.

Dinner at Golden Jug in Skadarlija, February 05, 2011.

Dinner at Golden Jug in Skadarlija, February 05, 2011.

Little Belgrade City Guide for Workshop Participants

Little Belgrade City Guide for Workshop Participants



Workshop Site

The workshop site is the building of the faculties of sciences of the University of Belgrade. It is located in the very city centre and close to Kalemegdan fortress, and the rivers Danube and Sava. The workshop site

is just 300m from the Knez Mihajlova street and the surrounding pedestrian zone, with a large number of impressive buildings and mansions built in XIX and XX century in the style of neoclassicism, academism, secession, and art-deco. Just 200m from the workshop site are remains of large Roman termes (built in III centrury) and 100m away is Sheikh Mustapha's turbeh (Turkish mausoleum; erected in XVIII century over the tomb of this religious figure), to name just a few intersting sights that are nearby.

Brief History of Belgrade

Belgrade, a city of very turbulent history, is one of the oldest cities in Europe. Its history lasts full 7000 years. The area around two great rivers, the Sava and the Danube has been inhabited as early as palaeolithic period. Remains of human bones and skulls of Neanderthals, found in Belgrade date back to the early Stone Age. The founding of Singidunum (the ancient name of Belgrade) is attributed to the Celtic tribe, the Scordiscs. Singidunum was mentioned for the first time in 279 B.C. The first part of the word - Singi - means "round" and dunum means "fortress" or "town". The Romans conquered Belgrade in the beginning of the I century A.D. and it has been under their rule for full four centuries. The Huns captured the town and completely destroyed it in 441. After the fall of the Huns, the town became a part of the Byzantine Empire in 454, but it was soon conquered by the Sarmatians, and later the Eastern Goths. In 488, it became a Byzantine town again. Around 630, the Serbian settlers come to this area. The town was first mentioned under the Slavic name Beograd (White Town - probably because of the walls made of white limestone) in 878. The Serbian rule over Belgrade began in 1284. but during some periods it was under Hungarians again. After almost a century of resisted sieges and attacks, Belgrade fell to Turks's rule in 1521. The town, getting more and more oriental look, counted in XVII population of 100000 and was the second-largest town in the Empire, right after Istanbul. The Austrians conquered Belgrade in 1688. When in 1739 it was captured again by the Turks, it was exposed to a heavy destruction. After two Serbian insurrections (started in 1804 in 1815) and the period of weaking of their power in Serbia, the Turks left Belgrade for good in 1867. In World War I, the Austrian army conquered the city in October 1915. The Serbian army and parts of the Allies' army liberated Belgrade in 1918. During WWI, Serbia lost 28% of its whole population, while Belgrade was the most destroyed town in Serbia. After the liberation, Belgrade became the capital of the newly-created Kingdom of the Serbs, Croats and Slovenes (later called Yugoslavia). In April 1941, Belgrade became the target of a terrible destruction by German air force. Belgrade also had to undergo losses in the Allies' bombing, especially in 1944. During World War II Belgrade lost about 50000 citizens and suffered inestimable damage. Belgrade was liberated by the units of the National Liberation Army of Yugoslavia and the Red Army on October 20, 1944. The monarchy in Yugoslavia was abolished in 1945 when the communist rule of Josip Broz Tito started. Thanks to a specific policy of Yugoslavia, Belgrade became an important international, political, cultural, sports, and economic center, linking East and West, North and South. Many unsolved national problems led to disintegration of Yugoslavia in 1991 and since 2006, the Republic of Serbia is independent state with Belgrade as its capital.

Briefly About Modern Belgrade

Belgrade is the capital and the largest city of Serbia. The city lies at the confluence of Sava and Danube rivers. With a population of almost two million, Belgrade is the third largest city in Southeastern Europe. The architecture of Belgrade is a mirror of different cultural and historical periods, influences and styles: from old Oriental influences, across baroque architecture, secession, academism and neoclassicism, socialist and industrial features from post WW2 period, to modern architecture and layout of New Belgrade with wide boulevards. Knez Mihajlova Street is the main walking street in Belgrade. It is a pedestrian zone, protected by law as one of the most valuable monumental complexes of the city. Belgrade has many beautiful parks and the biggest one is Kalemegdan, with an old fortress, comprising remains from Ancient and Byzantine times to Turkish and Austro-Ugrian periods. Belgrade has more than 20 theatres and two opera houses and it is home to a number of film, theater, and music festivals. There are many excellent restaurants, cafs and pubs, and British Times proclaimed Belgrade as Europe's best nightlife city.

Knez Mihajlova Street

Knez Mihajlova Street, pedestrian precinct and main city street, now protected by law, is one of the oldest and most valuable city environments, with a whole range of impressive buildings and town houses which sprung up at the end of the 1880's. It is generally believed that as early as Roman times this was the centre of the settlement of Singidunum, while during Turkish rule the streets went through the gardens, fountains and mosques that stood in this part of town. Today it is the main business area of Belgrade and the headquarters of many national institutions (such as the Serbian Academy of Science and Arts, Belgrade City Library and the Belgrade Cultural Centre).

Kalemegdan Park and Fortress

Kalemegdan is the core and the oldest section of the urban area of Belgrade and for centuries the city population was concentrated only within the walls of the fortress, thus its history, until most recent history, equals the history of Belgrade itself. The name Kalemegdan derives from two Turkish words, kale (fortress) and megdan (battleground) (literally, "battlefield fortress"). Kalemegdan fortress is the most important cultural-historical complex in the city, standing above the Sava-Danube confluence. Since its construction the Belgrade fortress has been constantly attacked and defended, destroyed and renovated. Chronicles trace a history of about 40 to 60 devastations of the fortress. The landscaping of the wide plateau around the fortress was begun on the order of Prince Mihailo Obrenovic after the fortress had been handed over from the Turks to the Serbs in 1867. and it was converted into a park in the 1880's. Today, Kalemegdan park is the largest and loveliest park in Belgrade with an area of 52 hectares. There is a number of monuments, Sahat Tower, the Military Museum, the statue of Belgrade Victor, the Zoo.

Serbian Alphabet

Serbian is a South Slavic language. Both Latin and Cyrillic alphabets are used to write Serbian. Serbian is an example of synchronic digraphia. The orthography, introduced by the language reform led by Vuk Karadi in mid XIX century, is very consistent: it is an approximation of the principle "one letter per sound". The following table gives 30 letters used in Serbian, both in Cyrillic and in Latin alphabet.

А а	Б б	В в	Г г	Д д	Ђ ђ	Е е	Ж ж	З з	И и	Ј ј	К к	Л л	Љ љ	М м
A a	B b	V v	G g	D d	Đ đ	E e	Ž ž	Z z	I i	J j	K k	L l	Lj lj	M m
Н н	Њ њ	О о	П п	Р р	С с	Т т	Ћ ћ	У у	Ф ф	Х х	Ц ц	Ч ч	Џ џ	Ш ш
N n	Nj nj	O o	P p	R r	S s	T t	Ć ć	U u	F f	H h	C c	Č č	Dž dž	Š š